PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-003284
(43)Date of publication of application : 06.01.1999

(51)Int.Cl. G06F 12/14
G06K 17/00
G06K 19/07

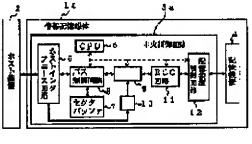
(21)Application number : 09-152687
(22)Date of filing : 10.06.1997

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : KORIN MEESON
SHINOHARA TAKAYUKI

(54) INFORMATION STORAGE MEDIUM AND ITS SECURITY METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To ensue the security function while keeping high versatility for an information storage medium by ciphering selectively the data received from a host device and decoding the stored data.



SOLUTION: When a host device 2 writes the new file data into an information storage medium 1a, a central controller 3a identifies whether the written data are the file management data or the file data based on the logical address value that is designated by the device 2. If the file management data are identified, a ciphering/decoding circuit 9 is not started and accordingly the data are not processed and stored in a storage 4 as they are. If the file data are identified, the circuit 9 is started to perform a ciphering operation based on the key information set by a ciphering/decoding key setting circuit 10. Then the ciphered data are written into a prescribed address of the storage 4 via a storage control circuit 12. This operation is reversed when the file data are read out of the medium 1a.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－3284

(43)公開日　平成11年(1999)１月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｅ
19/07		19/00	Ｎ

審査請求　未請求　請求項の数10　ＯＬ　（全７頁）

(21)出願番号　特願平9－152687

(22)出願日　平成９年(1997)６月10日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　コリン・メーソン
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　篠原　隆幸
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

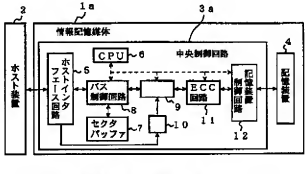
(74)代理人　弁理士　田澤　博昭　（外１名）

(54)【発明の名称】　情報記憶媒体およびそのセキュリティ方法

(57)【要約】

【課題】　情報記憶媒体に格納される貴重な個人情報がその汎用性故に容易に他人に読まれてしまうという課題があった。

【解決手段】　暗号化・復号化回路が機密性の高い個人情報であるファイルデータに対してのみ暗号化を実行し、既知であるファイル管理用のデータは平文のまま記憶装置に書き込みするように情報記憶媒体のセキュリティシステムを構築したので、この暗号方式で第三者による解読を困難にし高いセキュリティ機能が実現できる。



6：ＣＰＵ（中央処理装置）
9：暗号化・復号化回路（演算回路、第１演算回路）
１０：暗号化・復号化キー設定回路（演算回路、第２演算回路）

1

【特許請求の範囲】

【請求項１】　中央処理装置と、ホスト装置とデータ交換するインタフェース回路と、データを格納する記憶装置と、ホスト装置からのデータを選択的に暗号化し格納されたデータを復号化する演算回路とを備えた情報記憶媒体。

【請求項２】　演算回路はホスト装置からのデータをファイル単位で選択的に暗号化することを特徴とする請求項１記載の情報記憶媒体。

【請求項３】　ホスト装置からのコマンドに応じて演算回路を有効または無効にする選択手段を更に備えたことを特徴とする請求項１または請求項２記載の情報記憶媒体。

【請求項４】　中央処理装置と、ホスト装置とデータ交換するインタフェース回路と、データを格納する記憶装置と、必要的にデータの書き込み・読み出し双方時にそれぞれ暗号化・復号化する第１演算回路と、任意的にデータの書き込み・読み出しの双方時にそれぞれ暗号化・復号化する第２演算回路とを備えた情報記憶媒体。

【請求項５】　第２演算回路で行われる暗号化・復号化処理はその回路が更新またはリセットされるまで有効であることを特徴とする請求項４記載の情報記憶媒体。

【請求項６】　セクタデータ領域に書き込まれるデータを暗号化し、ファイル管理データに書き込まれるデータには暗号化しない情報記憶媒体のセキュリティ方法。

【請求項７】　ホスト装置からのコマンドに応じて書き込みデータに暗号化・復号化を実行することを特徴とする請求項６記載の情報記憶媒体のセキュリティ方法。

【請求項８】　書き込みデータには通常の暗号化・復号化を実行し、特殊キーデータの入力時には他の暗号化・復号化を実行する情報記憶媒体のセキュリティ方法。

【請求項９】　特殊キーデータの入力がホスト装置からのコマンドまたは情報記憶媒体に直接行われることを特徴とする請求項８記載の情報記憶媒体のセキュリティ方法。

【請求項１０】　特殊キーデータの入力が新たなキーデータ入力時または装置リセットないし電源オフまで有効とすることを特徴とする請求項９記載の情報記憶媒体のセキュリティ方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、情報処理装置の外部記憶媒体として使用される、フラッシュメモリ、ＥＥＰＲＯＭ、磁気ディスクメモリ等の記憶装置を搭載した情報記憶媒体およびそのセキュリティ方法に関するものである。

【０００２】

【従来の技術】電池による駆動を前提として携帯型情報端末機器の外部記憶媒体として、ＩＣカード、中でもフラッシュＡＴＡＰＣカード（以下、ＰＣカードと略称する）等の情報記憶媒体の普及が進んでいる。図７は、従来のフラッシュＡＴＡＰＣカード等の情報記憶媒体の機能ブロック図であり、図において、１ｅは情報記憶媒体、２はホスト装置、３ｅは中央制御回路、４はフラッシュメモリ、ＥＥＰＲＯＭ、磁気ディスクメモリ等の記憶装置、５はホストインタフェース回路、６はマイクロプロセッサ（ＭＰＵ）等の中央処理装置（ＣＰＵ）、７はセクタバッファ、８はバス制御回路、１１は誤り訂正コードすなわちＥＣＣ（Ｅｒｒｏｒ　Ｃｏｒｒｅｃｔｉｏｎ　Ｃｏｄｅ）回路、１２は記憶装置制御回路である。

2

【０００３】中央制御回路３ｅは、ホストインタフェース回路５、ＣＰＵ６、セクタバッファ７、バス制御回路８、ＥＣＣ回路１１、記憶装置制御回路１２から構成され、これらを１つの集積回路ＩＣチップに搭載することができる。また、ＥＣＣ回路１１はわずかなビットの誤りならば検出のみでなくその訂正も行う機能を有する。

【０００４】次に動作について説明する。この情報記憶媒体１ｅへのデータの書き込みについては、ホスト装置２が情報記憶媒体１ｅに新たなファイルデータを書き込む場合、ホスト装置２上のＤＯＳはファイル名、サイズ、作成日時等の情報からなるディレクトリエントリ情報と、そのファイルデータの論理的な格納場所を示すＦＡＴ（Ｆｉｌｅ　Ａｌｌｏｃａｔｉｏｎ　Ｔａｂｌｅ）情報を所定の論理アドレスに書き込んだ後、ファイルデータをデータ領域に書き込む。このとき、中央制御回路３ｅは、ホストインタフェース回路５を介して一時的にセクタバッファ７に蓄えられたデータをホスト装置２が指定する論理アドレス値に応じて平文のまま記憶装置４の所定の領域（ヘッダ領域、セクタデータ領域、ＥＣＣ領域）に書き込まれる。

【０００５】データの読み出しであるが、これはホスト装置２とホストインタフェース回路５を介してＣＰＵ６が通信して記憶装置４から格納データをセクタバッファ７を介して順次読み出していく。この際、格納データは平文のままなのでなんらデータ変換操作は伴わない。

【０００６】

【発明が解決しようとする課題】従来のＰＣカード等の情報記憶媒体は以上のように構成されているので、ハードディスク用のドライバソフトウェアによる読み書きが可能な汎用性の高い記憶媒体であるが、それゆえに情報記憶媒体１ｅ内に格納される貴重な個人情報も容易に他人に読まれてしまうという課題があった。この対策として、情報記憶媒体１ｅに格納される全ての情報に対して暗号化を実行し、セキュリティ機能を持たせることなどが考えられるが、このような暗号化機能を付加した情報記憶媒体１ｅのアクセスには専用のドライバソフトウェアが必須となり、その汎用性が損なわれてしまう。

【０００７】この発明は上記のような課題を解決するためになされたもので、ＰＣカード等の情報記憶媒体とし

ての汎用性の高さを保ちつつ、ユーザが他人に読まれたくないデータ（ファイル）のみを選択的に暗号化してフラッシュメモリ等の記憶装置に格納可能なセキュリティ機能付きの情報記憶媒体を得ることを目的とする。

【０００８】

【課題を解決するための手段】請求項１記載の発明に係る情報記憶媒体は、中央処理装置と、ホスト装置とデータ交換するインタフェース回路と、データを格納する記憶装置と、ホスト装置からのデータを選択的に暗号化し格納されたデータを復号化する演算回路とを備えたものである。

【０００９】請求項２記載の発明に係る情報記憶媒体は、演算回路はホスト装置からのデータをファイル単位で選択的に暗号化するものである。

【００１０】請求項３記載の発明に係る情報記憶媒体は、ホスト装置からのコマンドに応じて演算回路を有効または無効にする選択手段を更に備えたものである。

【００１１】請求項４記載の発明に係る情報記憶媒体は、中央処理装置と、ホスト装置とデータ交換するインタフェース回路と、データを格納する記憶装置と、必要的にデータの書き込み・読み出し双方時にそれぞれ暗号化・復号化する第１演算回路と、任意的にデータの書き込み・読み出しの双方時にそれぞれ暗号化・復号化する第２演算回路とを備えたものである。

【００１２】請求項５記載の発明に係る情報記憶媒体は、第２演算回路で行われる暗号化・復号化処理はその回路が更新またはリセットされるまで有効とするものである。

【００１３】請求項６記載の発明に係る情報記憶媒体のセキュリティ方法は、セクタデータ領域に書き込まれるデータを暗号化し、ファイル管理データに書き込まれるデータには暗号化しないものである。

【００１４】請求項７記載の発明に係る情報記憶媒体のセキュリティ方法は、ホスト装置からのコマンドに応じて書き込みデータに暗号化・復号化を実行するものである。

【００１５】請求項８記載の発明に係る情報記憶媒体のセキュリティ方法は、書き込みデータには通常の暗号化・復号化を実行し、特殊キーデータの入力時には他の暗号化・復号化を実行するものである。

【００１６】請求項９記載の発明に係る情報記憶媒体のセキュリティ方法は、特殊キーデータの入力がホスト装置からのコマンドまたは情報記憶媒体に直接行われるものである。

【００１７】請求項１０記載の発明に係る情報記憶媒体のセキュリティ方法は、特殊キーデータの入力が新たなキーデータ入力時または装置リセットないし電源オフまで有効とするものである。

【００１８】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態１．図１は、この発明の実施の形態１によるフラッシュＡＴＡＰＣカード等の情報記憶媒体の機能ブロック図であり、図において、１ａは情報記憶媒体、２はホスト装置、３ａは中央制御回路、４はフラッシュメモリ、ＥＥＰＲＯＭ、磁気ディスクメモリ等の記憶装置、５はホストインタフェース回路、６はマイクロプロセッサ（ＭＰＵ）等のＣＰＵ（中央処理装置）、７はセクタバッファ、８はバス制御回路、９は暗号化・復号化回路（演算回路、第１演算回路）、１０は暗号化・復号化キー設定回路（演算回路、第２演算回路）、１１は誤り訂正コードマなわちＥＣＣ回路、１２は記憶装置制御回路である。

【００１９】中央制御回路３ａは、ホストインタフェース回路５、ＣＰＵ６、セクタバッファ７、バス制御回路８、暗号化・復号化回路９、暗号化・復号化キー設定回路１０、ＥＣＣ回路１１、記憶装置制御回路１２から構成され、これらを１つの集積回路ＩＣチップに搭載することができる。

【００２０】図２は、一般的なディスクオペレーティングシステム（ＤＯＳ）でフォーマットされたＰＣカード等の情報記憶媒体１内部のデータ構造図である。このようにＤＯＳはその容量に応じて情報記憶媒体１のパーティショニング情報、ブート情報、およびファイル管理用の情報（ＦＡＴおよびディレクトリエントリ）を規定の領域に書き込むことによりフォーマットを実行する。これらの情報のうち、ファイル管理用の情報（ＦＡＴ（Ｆｉｌｅ　Ａｌｌｏｃａｔｉｏｎ　Ｔａｂｌｅ）およびディレクトリエントリ）は、ファイルデータの書き込みの都度その内容が更新される。

【００２１】さらに図３は、情報記憶媒体１のフラッシュメモリ等の記憶装置４に格納されるセクタデータの構成を示した図である。ヘッダ領域には一般的にそのセクタデータに付された論理セクタ番号が書き込まれ、読み出し時にＩＤ情報として参照される。セクタデータ領域には書き込むべきユーザデータが格納され、ヘッダ情報およびセクタデータに対するＥＣＣ（Ｅｒｒｏｒ　Ｃｏｒｒｅｃｔｉｏｎ　Ｃｏｄｅ）データがＥＣＣ領域に格納される。

【００２２】次に動作について説明する。先ず、データの書き込みについて説明する。図１において、ホスト装置２が情報記憶媒体１ａへ新たなファイルデータを書き込む場合、ホスト装置２上のＤＯＳには、ファイル名、サイズ、作成日時等の情報からなるディレクトリエントリ情報と、そのファイルデータの論理的な格納場所を示すＦＡＴ（Ｆｉｌｅ　Ａｌｌｏｃａｔｉｏｎ　Ｔａｂｌｅ）情報を所定の論理アドレスに書き込まれた後に、ファイルデータがデータ領域に書き込まれる。

【００２３】このとき、中央制御回路３ａでは、ホスト装置２により指定された論理アドレス値に基づいて、書

き込みデータがファイル管理用データかファイルデータかどうかを識別される。これが前者のファイル管理用データの場合には、暗号化・復号化回路９が起動せず未処理のままで記憶装置４に格納され、一方、後者のファイルデータの場合には、暗号化・復号化回路９が起動され、暗号化・復号化キー設定回路１０に設定されたキー情報を用いて暗号化・復号化回路９に暗号化演算を行わせ、その暗号化データを記憶装置制御回路１２を介して記憶装置４の所定のアドレスに書き込む。以上の判断・指令は、図２の破線を経由してＣＰＵ６が行うものである。

【００２４】次に、情報記憶媒体１ａからのデータの読み出しであるが、これは上述の逆の操作を行えばよい。すなわち、ホスト装置２が指定した論理アドレス値に基づいて、記憶装置４からの読み出しデータがファイル管理用のデータかファイルデータかを識別し、前者には復号化をかけずに後者のみに復号化をかけるように選択的に暗号化・復号化回路９を起動させ、暗号化・復号化キー設定回路１０のキー情報を用いて復号化演算を行い、これによりファイルデータ部分のみを復号化してホスト装置２に読み出すものである。

【００２５】以上のように、この実施の形態１によれば、暗号化・復号化回路９はファイルデータのみに対して暗号化を実行し、既知であるファイル管理用のデータは平文のまま書き込みすることにより、第三者によるこの暗号方式の解読を困難にすることができるのでより高いセキュリティ機能が実現できるという効果が得られる。

【００２６】実施の形態２．図４は、この発明の実施の形態２によるフラッシュＡＴＡＰＣカード等の情報記憶媒体の機能ブロック図である。図において、１ｂは情報記憶媒体、３ｂは中央制御回路、１３はデータ転送バス切り替え回路、Ｓ１，Ｓ２はスイッチである。その他の構成は、前記実施の形態１と同様であるから同一部分には同一符号を付して重複説明を省略する。データ転送バス切り替え回路１３は、暗号化・復号化回路９を有効とする場合にはスイッチＳ１，Ｓ２はそれぞれＰ１，Ｐ３に接続され、これを無効とする場合にはスイッチＳ１，Ｓ２はそれぞれＰ２，Ｐ４に接続されるように作動するものである。

【００２７】この実施の形態２では、拡張コマンドによりファイル毎に暗号化の実行を選択可能とした。このようなファイル単位での暗号化の実行を選択できるようにするために、下記の３つの拡張コマンド（１）～（３）を定義する。

【００２８】（１）　暗号化キーロードコマンド
暗号化・復号化のためのキーデータを暗号化・復号化回路９にロードするコマンド。
（２）　暗号化付ライトセクタコマンド
ホスト装置２よりロードされたキーデータにより暗号化されたデータを記憶装置４に書き込む。
（３）　復号化付リードセクタコマンド
ホスト装置２よりロードされたキーデータにより、暗号化されたデータに対し復号化処理を実行し読み出すコマンド。

【００２９】暗号化付ライトセクタコマンド、または復号化付リードセクタコマンドを発行すると、ホスト装置２側のドライバソフトウェアは、その都度暗号化キーコマンドで設定すべき暗号データの入力を要求するように設計されている。したがって、これら暗号化・復号化付ライト・リードコマンド実行時は、そのデータ（ファイル）に固有の暗号化・復号化キーを組み合わせて入力することにより、通常のリードセクタコマンドでは読み出しができない、セキュリティの高いデータ記憶システムが実現可能となる。

【００３０】以下、このようにファイル単位での選択的な暗号化・復号化処理を実現する方法について説明する。図４において、データ転送バス切り替え回路１３は、ホスト装置２の暗号化・復号化付ライト・リードコマンド実行時のみスイッチＳ１，Ｓ２をＰ１，Ｐ３に接続して暗号化・復号化を有効にし、通常のライト・リードセクタコマンド実行時は暗号化・復号化回路を無効にするようにスイッチＳ１，Ｓ２をＰ２，Ｐ４に接続して、回路内部のデータ転送ルートの切り替えを実施する。

【００３１】以上のように、この実施の形態２によれば、ホスト装置２が上述の拡張コマンド（１）～（３）を発行した時のみ暗号化・復号化回路が有効化され、ファイル単位の暗号化が可能となるので、そのファイルデータに固有の暗号化・復号化キーを組み合わせて入力することにより、通常のリードセクタコマンドでは読み出しができない、セキュリティの高いデータ記憶システムが実現できるという効果が得られる。

【００３２】実施の形態３．図５は、この発明の実施の形態３によるフラッシュＡＴＡＰＣカード等の情報記憶媒体の機能ブロック図である。図において、１ｃは情報記憶媒体、３ｃは中央制御回路、１５はデフォルトキー入力装置であり、その他の構成は、前記実施の形態１と同様であるから同一部分には同一符号を付して重複説明を省略する。

【００３３】次に動作について説明する。ＰＣカード等の情報記憶媒体１に格納されるすべてのファイルデータに対して暗号化が実行される。すなわち、通常のライト・リードセクタコマンドの実行時は、暗号化・復号化キー設定回路１０にデフォルトキー入力装置１５より与えられるデフォルトのキーデータにより暗号化・復号化が実行される。また、拡張コマンドである暗号化・復号化付ライト・リードコマンド実行時のみ、組み合わせて実行される暗号化・復号化キーロードコマンドにより設定された固有のキーデータが、暗号化・復号化キー設定回

路10により暗号化・復号化回路9に与えられ、暗号化・復号化が実行される。

【0034】以上のように、この実施の形態3によれば、拡張コマンド実行時のみ特別のキーデータによる暗号化・復号化回路を実行し、通常のライト・リードセクタコマンド実施時にはデフォルトのキーデータによる暗号化・復号化を実施するように構成したため、暗号化・復号化回路9部分の共通化が可能となり、小さな回路規模でファイル単位での選択的な暗号化・復号化が可能な高いセキュリティ機能を有するという効果が得られる。

【0035】また、このデフォルトキー入力装置15を上述の実施の形態2の場合に適用したものが変形例として考えられ、これは図6の情報記憶媒体1dに対応するものである。この変形例によれば、前記拡張コマンド実行時のみ特別のキーデータによる暗号化・復号化回路を実行し、通常のライト・リードセクタコマンド実施時にはデフォルトのキーデータによる暗号化・復号化を実施するように構成したことに加えて、ホスト装置2が上述の拡張コマンド（1）～（3）を発行した時のみデータ転送バス切り替え回路13が起動して暗号化・復号化回路が有効化され、ファイル単位の暗号化が可能となるので、そのファイルデータに固有の暗号化・復号化キーを組み合わせて入力することにより、通常のリードセクタコマンドでは読み出しができないようにも構成することができるので、更にセキュリティの高いデータ記憶システムが実現できるという効果がある。

【0036】実施の形態4．前記実施の形態3では、拡張コマンドである暗号化・復号化付ライト・リードセクタコマンド実行の度に、組み合わせて発行される暗号化・復号化キーロードコマンドにより、そのファイルに固有のキーデータを設定して暗号化・復号化を実行した。この実施の形態4では、暗号化キーロードコマンドによりロードされたキーデータを、新たなキーデータが入力されるまで、またはリセットないし電源オフされるまで有効とし、通常のライト・リードセクタコマンド実行時もこのキーデータによる暗号化・復号化が実行される例を示す。ここでは、デリートキーなるオプションコマンドにより、上述のロード済みのキーデータを消去し、デフォルトのキーデータが有効となる。

【0037】以上のように、この実施の形態4によれば、暗号化キーロードコマンドによりロードされたキーデータを、新たなキーデータが入力されるまで、またはリセットないし電源オフされるまで有効としたので、簡易な構成で高いセキュリティを有する効果がある。

【0038】

【発明の効果】以上のように、請求項1記載の発明によれば、演算回路がホスト装置からのデータを選択的に暗号化し格納されたデータを復号化するように構成したので、ホスト装置からのデータをその秘密性に応じて選択的に暗号化・復号化を施すことができ、これにより汎用性の高い情報記憶媒体であっても格納される貴重な情報に対してセキュリティをかけることができる効果がある。

【0039】請求項2記載の発明によれば、演算回路はホスト装置からのデータをファイル単位で選択的に暗号化するように構成したので、ファイル管理用のデータか機密性の高いファイルデータかその種類・用途に応じて暗号化してセキュリティをかけることができる効果がある。

【0040】請求項3記載の発明によれば、選択手段がホスト装置からのコマンドに応じて演算回路を有効または無効にするように構成したので、通常のホスト装置のリードコマンドでは読み出しができないように設定することができ、したがってセキュリティの高いデータ記憶システムとすることができる効果がある。

【0041】請求項4記載の発明によれば、第1演算回路が必要的にデータの書き込み・読み出し双方時にそれぞれ暗号化・復号化し、しかも第2演算回路が任意的にデータの書き込み・読み出しの双方時にそれぞれ暗号化・復号化するように構成したので、通常のホスト装置からのコマンドでは第1演算回路が動作してデータを暗号化・復号化し、拡張コマンドのときのみ第2演算回路が動作して他の暗号化・復号化を行うように設定することができるので、第1および第2演算回路の共通化が可能となり、小規模回路で選択的な暗号化・復号化が可能なセキュリティ機能を付加できる効果がある。

【0042】請求項5記載の発明によれば、第2演算回路で行われる暗号化・復号化処理はその回路が更新またはリセットされるまで有効とするように構成したので、簡易なシステムで高いセキュリティを実現する効果がある。

【0043】請求項6記載の発明によれば、セクタデータ領域に書き込まれるデータを暗号化し、ファイル管理データに書き込まれるデータには暗号化しないように構成したので、個人情報などの機密性の高いデータに対してより高いセキュリティを持たせることができる効果がある。

【0044】請求項7記載の発明によれば、ホスト装置からのコマンドに応じて書き込みデータに暗号化・復号化を実行するように構成したので、通常のホスト装置からのリードセクタコマンドでは読み出しができないセキュリティの高いデータ記憶システムを実現できる効果がある。

【0045】請求項8記載の発明によれば、書き込みデータには通常の暗号化・復号化を実行し、特殊キーデータの入力時には他の暗号化・復号化を実行するように構成したので、通常の暗号化・復号化と特殊キーデータの入力時の他の暗号化・復号化を共通の手段で行うことができる。これにより装置規模を縮小できる効果がある。

【0046】請求項9記載の発明によれば、特殊キーデ

ータの入力がホスト装置からのコマンドまたは情報記憶媒体に直接行われるように構成したので、ホスト装置および情報記憶媒体の両方面からセキュリティを実行できる効果がある。

【００４７】請求項１０記載の発明によれば、特殊キーデータの入力が新たなキーデータ入力時または装置リセットないし電源オフまで有効とするように構成したので、簡易なセキュリティソフトウェアの設定で機密保持ができる効果がある。

【図面の簡単な説明】

【図１】　この発明の実施の形態１による情報記憶媒体の機能ブロック図である。

【図２】　この発明の実施の形態１による情報記憶媒体のＤＯＳフォーマット後のデータ構造図である。

【図３】　この発明の実施の形態１による情報記憶媒体＊のデータ構成図である。

【図４】　この発明の実施の形態２による情報記憶媒体の機能ブロック図である。

【図５】　この発明の実施の形態３による情報記憶媒体の機能ブロック図である。

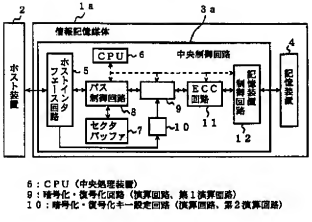
【図６】　この発明の実施の形態３の変形例による情報記憶媒体の機能ブロック図である。

【図７】　従来の情報記憶媒体の機能ブロック図である。

【符号の説明】

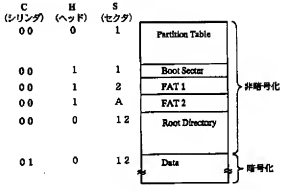
１ａ～１ｅ　情報記憶媒体、２　ホスト装置、４　記憶装置、６　ＣＰＵ（中央処理装置）、９　暗号化・復号化回路（演算回路、第１演算回路）、１０　暗号化・復号化キー設定回路（演算回路、第２演算回路）。

【図１】

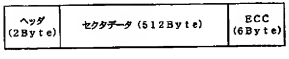


6：ＣＰＵ（中央処理装置）
9：暗号化・復号化回路（演算回路、第１演算回路）
１０：暗号化・復号化キー設定回路（演算回路、第２演算回路）

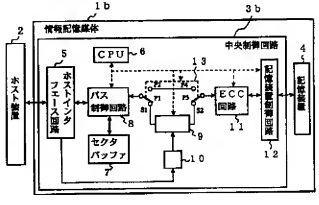
【図２】



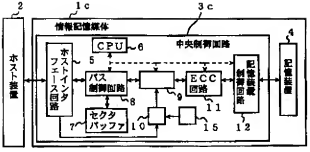
【図３】



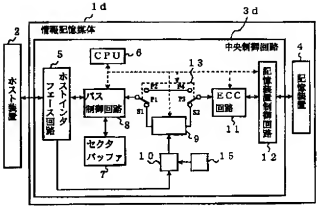
【図４】



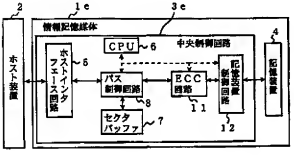
【図5】


2
1c
3c
情報記憶媒体
ホスト装置
CPU
6
中央制御回路
ホストインタフェース回路
5
バス制御回路
8
ECC回路
11
セクタバッファ
7
9
10
15
記憶装置制御回路
12
4
記憶装置

【図6】


1d
3d
2
情報記憶媒体
中央制御回路
ホスト装置
5
CPU
6
13
ホストインタフェース回路
バス制御回路
8
ECC回路
11
セクタバッファ
7
9
10
15
記憶装置制御回路
12
4
記憶装置

【図7】


2
1e
3e
情報記憶媒体
ホスト装置
CPU
6
中央制御回路
ホストインタフェース回路
5
バス制御回路
8
ECC回路
11
セクタバッファ
7
記憶装置制御回路
12
4
記憶装置